Available Online at www.ijcsmc.com

International Journal of Computer Science and Mobile Computing

A Monthly Journal of Computer Science and Information Technology

ISSN 2320–088X

IJCSMC, Vol. 2, Issue. 4, April 2013, pg.402 – 408

RESEARCH ARTICLE

Modified Security Frame Work for PIR Cloud Computing Environment

J. Sinduja[1], S. Prathiba[2]
[1]Department of Computer Science and Engineering, Bharat University, Chennai, India
[2]Department of Computer Science and Engineering, Bharat University, Chennai, India

Abstract— Computational Private Information Retrieval (cPIR) protocols allow a client to retrieve one bit from a database, without the server inferring any information about the queried bit. These protocols are too costly in practice because they invoke complex arithmetic operations for every bit of the database. Our approach assumes a disk-based architecture that retrieves one page with a single query. Our results indicate that pCloud reduces considerably the query response time compared to the traditional client/server model, and has a very low communication overhead. Additionally, it scales well with an increasing number of peers; achieving a linear speedup Data outsourcing is a new paradigm in which a third party provides storage services. This is more cost effective for the user as there is no need of purchasing expensive hardware and software for data storage. Before data out sourcing can become viable, the data provider needs to guarantee that the data is secure, be able to execute queries on the data, and the results of the queries must also be secure and not visible to the data provider. Data encryption, Homomorphic Encryption, Secret Sharing algorithms and Private Information Retrieval (PIR) are the techniques widely used for secure data outsourcing. CIA (Confidentiality, Integrity and Availability) are the challenging issues associated with data storage management with/without data outsourcing. In this paper the performance of two secret sharing algorithms are compared. The Shamir's secret sharing algorithm and Rabin's Information Dispersal Algorithm (IDA) are implemented in a private cloud setup using the Open Stack Cloud framework.

Key Terms: - Data Security; Cloud; Secret sharing; Information Dispersal

Full Text: http://www.ijcsmc.com/docs/papers/April2013/V2I42013104.pdf

© 2013, IJCSMC All Rights Reserved